Areas for Clarity: Enhanced Weapons and Security Event Notifications Rule

Date: 05/02/2023

Regarding Incorporation of Part 95-Related Reporting Requirements

Adding these new reporting requirements under Part 73 has created substantial confusion.

- It is unreasonable to assume that a licensee implementing a program to meet Part 95 will be aware of additional reporting requirements buried in Subpart T to Part 73.
- The term contraband has been expanded in 10 CFR 73.2 to include electronic devices and electronic media, resulting in a number of questions about how requirements in Subpart T can be met. For example, the four-hour notification requirement in 10 CFR 73.1200(f)(1)(vii) includes, "The attempted introduction of contraband into the Category I or II quantity of SSNM, Category II quantity of SNM, SNF, or HLW being transported."
- Confusion exists where licensees may be subject to Part 95, but where NRC may have established an arrangement for another federal agency (e.g., Department of Energy) to act as the facility's cognizant security agency. Specifically, for reports regarding Part 95 information that are codified in Part 73, would the licensee submit reports to the NRC, the CSA, or both?

Part 95 already contains reporting requirements consistent with the performance objectives of that regulation.

- Security programs implemented to meet Part 95 for the protection of information against unauthorized disclosure are distinctly different from security programs implemented to meet Part 73 for the protection of plants and materials against theft or sabotage. Part 95 and Part 73 should continue to contain separate and distinct reporting requirements consistent with the performance objectives of those regulations.

NRC should act promptly to eliminate this unnecessary intermingling of Part 95 and Part 73.

- Prompt action is warranted given the final rule has been issued and licensees must begin implementation, and given the substantial confusion created.

Reporting requirements regarding information protected under 10 CFR Part 95 should be removed from Part 73 and should, as determined necessary, be addressed through a separate rulemaking.

Regarding 10 CFR 73.17, "Firearms Background Checks for Armed Security Personnel"

- Firearm training questions:
  - Do these requirements cover the on-boarding process and new hire training of employees that are intended to join the security force but do not have official duties or qualifications associated with the security force?
  - Does the periodic training include security staff that have access to enhanced weapons via keys and armory combos, but do not currently receive annual training in the same format as uniformed officers?
- Firearm Background questions:
  - Does this requirement include employees that are in the on-boarding process that are intended to join the security force but do not have official duties or qualifications associated with the security force?

- There appears to be a conflict between § 73.17(b)(9)(ii) and § 73.17(q)(5)
  - (q)(5) says a background check may be transferred to another licensee.
  - (b)(9)(ii) says a new background check must be completed if they transferred from a different licensee.

Regarding 10 CFR Part 73, Subpart T, "Security Notifications, Reports, and Recordkeeping"

Contraband Definition

Background: The term contraband as used in Nuclear Power Plants (NPPs) and Category I (CAT I) fuel cycle facilities includes items for which a search is performed to prevent unauthorized introduction into a controlled area (e.g., the protected area of a nuclear power plant). RG 5.76 and NEI 03-12 identically define contraband as *firearms, explosives, incendiary devices, or other items that may be carried or concealed by personnel, packages, materials or vehicles and could be used to commit radiological sabotage*. Licensees have used other terms (e.g., prohibited items, controlled items) to refer to a population of items that are banned from introduction into a controlled area, but for which as search is not performed in order to prevent the introduction of items that could be used to commit radiological sabotage.

The definition of contraband added to 10 CFR 73.2 has three component parts. Clarity is needed regarding each component.

1) *Contraband* means unauthorized firearms, explosives, incendiaries, or other dangerous materials (e.g., disease causing agents), which are capable of causing acts of sabotage against a licensed facility or licensed radioactive material, as specified under 42 U.S.C. 2284.
   - Industry reads this statement to be consistent with the current definition of contraband as defined in RG 5.76 and NEI 03-12.
   - NRC should clarify that the expression “diseasing causing agents” is not applicable to NPPs or CAT I facilities (and may not be applicable to any licensee subject to Part 73).
     - Addition of disease causing agents or other items that do not fit the traditional definition of contraband (e.g., as defined in RG 5.76 or NEI 03-12) could require the introduction of new search systems and processes that were not accounted for in the regulatory analysis performed for this rulemaking.
   - Should NRC affirm that disease causing agents are contraband:
     - What does compliance look like for a successful strategy for licensees to identify and prevent these from entering a PA, VA, MAA or CAA?
2) For licensees that possess or conduct activities involving classified national security information or classified Restricted Data (RD) as defined in § 95.5 of this chapter, contraband also means unauthorized electronic devices or unauthorized electronic media that are capable of facilitating acts of espionage; unauthorized communication, transmission, disclosure, or receipt of RD; or tampering with RD, pursuant to 18 U.S.C. 793 or 42 U.S.C. 2274-2276, respectively.
   - For the reasons discussed above, this requirement should have been addressed in a rulemaking to revise 10 CFR Part 95.
   - These items do not fit the historical definition of contraband, and facilities do not search for these items in order to prevent the introduction of items that could be used to

commit radiological sabotage. Identifying these items as contraband could require the introduction of new search systems and processes that were not accounted for in the regulatory analysis performed for this rulemaking.

3) Contraband items are banned from a licensee's protected area, vital area, materials access area, or controlled access area.
    - The industry interprets this to mean that contraband is banned; and not to mean all things licensees ban or prohibit from a PA, VA, MAA or CAA is contraband.

Time of Discovery

Time of discovery means the time at which a cognizant individual observes, identifies, or is notified of a security-significant event or condition. A cognizant individual is considered anyone who, by position, experience, and/or training, is expected to understand that a particular condition or event adversely impacts security.

- Industry interprets this definition as equivalent to the definition currently found in RG 5.76 and NEI 03-12. (See NRC comments at 76FR6213 dated February 3, 2011).
- Licensee security plans or other implementing guidance would provide specificity regarding what constitutes a cognizant individual.

15-Minute Notification Requirements

- Notification of Hostile Action events:
    - The industry did find clarification within the Regulatory Guides that the security event notification should not take precedence over request for immediate LLEA assistance, initiation of a contingency response, or notification of State officials required under the licensee's Emergency Response Plan.
    - However, a question still exists as it pertains to notification to the HOC.
        - Discovery of the event is T=0
        - Classification process complete is T+15
        - Notification to State officials required under the licensee's Emergency Response Plan is T+30
        - Notification to the HOC for EAL classification under 50.72 is immediately after T+30, but no longer than T+60 minutes from event classification (T+75)
        - The industry desires to make one notification to the HOC during a security related event that also results in an EAL classification. The industry's position is that the time requirement from event classification to NRC HOC notification IAW 50.72 requirements is adequate. The information required for reporting the new security event notification is encompassed within the 50.72 notification requirement, and the Security event notification required at T+60 is 15 minutes earlier than required per 50.72.
- There is a discrepancy between the 15-minute notification requirement for hostile action and a 4-hour notification requirement for contraband.
    - RG 5.62, page 24 provides examples of "hostile action":
      "(4) The discovery of unauthorized explosive materials, incendiary materials, or an improvised explosive device within the licensee's **site boundary**" is provided as an example.
    - "Incendiary" is also used in the definition of contraband.
        - § 73.1200(e)(1)(iii) requires a 4-hour notification of the introduction of contraband into a **PA.**

- The industry desires clarification on the basis for a shorter reporting requirement related to incendiary devices within a site boundary, versus a longer reporting requirement for incendiary devices with a PA.

"Hostile threat" versus "Hostile Action" terminology in 73.1200(b)(3)(ii)(A):

- The industry interprets the use of both terms to mean the same.

Security Events per 73.1200(c)(1)(i)(C) & (D)

- The industry interprets this to EXCLUDE events due to Human Performance Errors

Media Inquiries Per 73.1200(e)(3)(i)

- This requirement appears to overlap with 50.72 requirements.
- The industry desires to understand if this is intended to be a separate reporting requirement from 50.72, or if the desire is to report for an inquiry and one for potential media coverage.

Determination of malevolent intent

- RG 5.62, page 21, states that the NRC's position that only government officials have the necessary resources and qualifications to determine whether malevolent intent was present in a security event. Such Government officials include, but are not limited to, the NRC Office of Investigations (OI); the intelligence community; or a Federal, State, or local law enforcement agency.
    - The industry desires an understanding for the basis of this position, as this is a change in philosophy on the way the industry has been operating and could impose a significant increase in resources from our agreement LLEAs.
    - Suspicious activities where LLEA has determined no malevolent intent existed prior to the 4-hour reporting requirement, the industry interprets this to mean that a report and subsequent retraction is not warranted.

10 CFR 73.1200(e)(1)(v) discovery that a weapon that is authorized by the licensee's security plan is lost or uncontrolled within a PA, VA, or MAA

- The industry desires discussion on "not in possession." Is there a line of sight and/or timeframe associated with this new reporting requirement?

10 CFR 73.1215(c)(1)(iii) If a suspicious activity report results in a LLEA response the licensee must notify the NRC in accordance with the requirements of § 73.1200 of this part.

- **RG.5.87 Page 12 Notification Process: "**This LLEA would typically have jurisdiction over the physical location of the facility or material. For shipments this would be the physical location of the shipment when the suspicious activity occurred. <u>If a licensee has an existing LLEA point of contact, then the licensee should confirm if this LLEA point of contact</u> is also appropriate for receiving reports of suspicious activities. If not appropriate, then the licensee should coordinate with the LLEA to update its point of contact. For reports of suspicious activities for shipments the appropriate LLEA contact phone numbers along the shipment route are specified in the NRC-reviewed route approval document (e.g., a state police force communications center)."

- The industry interprets LLEA having jurisdiction over the physical location of the facility or material as the LLEA that the licensee has established agreement in accordance with § 73.55 (k)(9) and intends to implement as such.

10 CFR 73.1215(d)(iii) Challenges to the licensee's security systems and procedures

- RG 5.87 section 5.2 page 17 examples:
  - Unauthorized tests or challenges of security screening, detection, and assessment systems. This reporting applies to both interior and exterior security systems.
    - Licensees interpret this to mean willful or intentional unauthorized challenges, not events due to HU errors.

References

Regulatory Guide (RG) 5.76, "Physical Protection Programs at Nuclear Power Reactors," Revision 2, dated 2020

Nuclear Energy Institute (NEI) 03-12, "Template for the Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, [and Independent Spent Fuel Storage Installation Security Plan]," Revision 7, dated October 2011; and Revision 7.1 dated January 2018